

NOT FOR PUBLICATION

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

LEGEND BIOTECH USA INC.,

Plaintiff,

v.

LIANXING LIU,

Defendant.

Case No. 2:23-cv-02965-BRM-LDW

AMENDED OPINION

MARTINOTTI, DISTRICT JUDGE

Before the Court is Plaintiff Legend Biotech USA’s (“Plaintiff”) Motion for Preliminary Injunction to compel Defendant Lianxing Liu (“Defendant”) to submit all devices, online accounts, and hard copy documents in his possession, custody, and control to a forensic vendor for forensic inspection. (ECF Nos. 29–31.) Defendant filed an opposition (ECF No. 40), and Plaintiff filed a reply (ECF No. 42). Having reviewed the submissions filed in connection with the Motion and having declined to hold oral argument pursuant to Federal Rule of Civil Procedure 78(b), for the reasons set forth below and for good cause having been shown, Plaintiff’s Motion for Preliminary Injunction is **GRANTED**.

I. BACKGROUND

A. Factual History

Plaintiff is a biotechnology company developing cell-editing therapies for cancer and other diseases based on DNA, RNA, plasmid, and amino acid sequences. (ECF No. 1 ¶¶ 3–6.) Plaintiff’s cell-editing therapies are known as CAR-T cell therapies. (*Id.* ¶ 6.) In order to protect proprietary information pertaining to the therapies, Plaintiff implements a variety of security measures,

including Data Loss Prevention and Insider Threat Management applications to flag outgoing emails and file transfers which contain potentially proprietary or confidential information. (*Id.* ¶ 7.) When such information is flagged by the applications, it is then quarantined for further review. (*Id.*) Plaintiff also uses programs to sweep the internet for potential proprietary and confidential information. (*Id.*) All of Plaintiff's employees must "read and agree to confidentiality obligations, a code of conduct, a data protection policy, a data handling policy, and media retention and destruction policies as a condition of their employment." (*Id.*)

On August 25, 2021, Plaintiff sent Defendant an offer letter for employment, and Defendant began working for Plaintiff shortly thereafter. (*Id.* ¶ 14.) As part of Defendant's onboarding, he signed an "Intellectual Property Rights Assignment, Non-Competition and Confidentiality Agreement" (*id.*) in which he agreed not to use Plaintiff's confidential information without written consent (ECF No. 1-3 § 1.2), and to return Plaintiff's documents and property upon request during his employment (*id.* § 5). Shortly after beginning his employment with Plaintiff, Defendant allegedly began emailing Plaintiff's trade secrets and confidential information to his personal Gmail account, lianxing.liu@gmail.com. (ECF No. 1 ¶ 18.) During his employment, he also engaged in conversations with other cell therapy companies competing with Plaintiff about alternative employment. (*Id.* ¶¶ 35–36.)

On May 10, 2023, Plaintiff, through its Data Loss Prevention system, flagged a file Defendant had sent to his personal email account from his company email account. (*Id.* ¶ 19.) Plaintiff determined this file contained its trade secrets and confidential information, specifically, "████████ for [Plaintiff]'s proprietary ██████████ for a clinical product candidate." (*Id.*) The file was on Plaintiff's vendor portal to which Defendant did not have download access. (*Id.*) Defendant titled the email sent to his personal email address as "Notes LL.docx." (*Id.*)

After this email was flagged, Plaintiff obtained email logs of all emails sent from Defendant's company email account to his personal email account. (*Id.* ¶ 20.) These logs showed Defendant had sent confidential internal presentations, research data, [REDACTED]

[REDACTED] to his personal email account. (*Id.* ¶ 21.) Plaintiff met virtually with Defendant on May 11, 2023 through a human resources representative, where Defendant was asked to access his personal email account via his work laptop. (*Id.* ¶ 22.) Defendant claimed he did not know how to access his personal email account from his work laptop, which prompted Plaintiff's IT representative to instruct Defendant on how to do this. (*Id.*) Defendant alleges that during this meeting, Plaintiff threatened criminal action against Defendant. (ECF No. 40 at 2–3.) Once Defendant gained access to his personal email account, Defendant showed the account to Plaintiff. (ECF No. 1 ¶ 22.) Plaintiff then directed him to run several searches within his personal email account for any emails sent from Plaintiff's email domain. (*Id.*) The searches revealed more than one hundred emails containing confidential and trade secret data, and Plaintiff instructed Defendant to delete all confidential data discovered during the searches. (*Id.*) During this meeting, Plaintiff also discovered Defendant was seeking employment with Plaintiff's competitors by offering to help such competitors develop cell therapy businesses and products related to the trade secrets Defendant allegedly took. (ECF No. 31 at 8.) At the meeting, Plaintiff asked Defendant to share the desktop from his personal laptop to confirm Plaintiff's confidential files were not saved locally on the computer. (*Id.* ¶¶ 23–24.) Defendant claimed he was unable to share the screen, leading Plaintiff to request Defendant bring his laptop to its Piscataway, New Jersey office on May 17, 2023. (*Id.* ¶¶ 24–26.)

On May 17, 2023, Defendant produced his laptop to Plaintiff, and Plaintiff discovered the “trash” on the laptop was emptied on May 16, 2023, shortly after Plaintiff had requested Defendant

bring his laptop to the office. (*Id.* ¶ 26.) At the meeting, Plaintiff searched Defendant's personal email to confirm the documents deleted on May 11, 2023 were gone, and searched all files in the computer to confirm no files obviously belonged to Plaintiff. (*Id.*) Plaintiff found no files belonging to it, although certain files had been renamed. (*Id.*)

On May 19, 2023, Plaintiff reclaimed Defendant's work laptop, which underwent forensic analysis. (*Id.* ¶ 27.) On May 22, 2023, Plaintiff reviewed all emails Defendant had sent from his company email account, finding more "non-public [REDACTED] for [Plaintiff's] proprietary therapeutic delivery platform, internal protocols for testing, and templates for further studies" were sent to his personal email account under titles such as "Notice." (*Id.* ¶ 28.) On May 23, 2023, Plaintiff demanded Defendant produce his personal laptop and phone for imaging, and on May 24, 2023, Plaintiff imaged Defendant's "Macbook Pro, his Apple iPhone 11 (including his WeChat and other messaging platform files), his personal Gmail account, his iCloudsync data, and his personal Google Drive account that is associated with his personal Gmail account." (*Id.* ¶ 29.) During this meeting, Defendant was not represented by counsel or given an *Upjohn* warning¹. (ECF No. 40 at 8.) Forensic analysis also later revealed Defendant had photographs of Plaintiff's potentially confidential information, and that he may possess additional devices with relevant data. (ECF No. 1 ¶ 38.) In particular, the analysis revealed "Defendant had stored on his personal iPhone multiple photos of [Plaintiff's] slides marked as privileged, confidential, and for internal use only" among other documents stored on personal devices. (ECF No. 31 at 7–8.)

¹ An *Upjohn* warning is given by corporate counsel to employees of the company to clarify that their representation is of the company, and not of the individual. Such warnings are generally given to notify individuals that privilege over communications between the company and the individual is held by the company. *Heritage Pharm., Inc. v. Glazer*, Civ. A. No. 16-8483, 2019 WL 9309180, at *3 n.1 (D.N.J. Mar. 1, 2019); *Utesch v. Lannett Co., Inc.*, Civ. A. No. 16-5932, 2020 WL 7260775, at *8 n.5 (E.D. Pa. Dec. 9, 2020); *In re Processed Eggs Prods. Antitrust Litig.*, MDL No. 08-02002, 2014 WL 6388436, at *11 (E.D. Pa. Nov. 17, 2014).

On May 25, 2023, Plaintiff terminated Defendant's employment, and Defendant signed a "Certification of Document Destruction" in which he indicated he had reviewed and agreed to abide by "the Record Management Policy, the Global Data Privacy Policy, the Global Data Handling and Classification Policy, and the Data Handling and Classification Standard Operating Procedures" which outline procedures for classifying and assessing the risk and impact level of information. (ECF No. 1 ¶ 30.) He also signed documents making various admissions, including that he "exceeded the scope of his authority to access and use the computer systems of [Plaintiff] and its affiliates." (*Id.*)

B. Procedural History

Plaintiff filed its Complaint on May 31, 2023. (ECF No. 1.) Along with its Complaint, Plaintiff also filed a motion for a Temporary Restraining Order ("TRO"). (ECF No. 1-7.) The Court held a hearing on Plaintiff's motion for a TRO on June 1, 2023 (ECF No. 5), at which time Defendant consented to the entry of a TRO barring his access to Plaintiff's confidential and secret information in his possession, requiring him to preserve and maintain all such information in his possession, and setting an expedited discovery schedule. (ECF No. 6.) On June 6, 2023, counsel filed notices of appearance on behalf of Defendant. (ECF Nos. 10, 11.) On August 1, 2023, through counsel, Defendant filed an Answer to the Complaint. (ECF No. 26.)

On August 28, 2023, Plaintiff filed the present Motion for Preliminary Injunction. (ECF Nos. 29–31.) On September 18, 2023, Defendant filed an opposition. (ECF No. 40.) On October 2, 2023, Plaintiff filed a reply. (ECF No. 42.)

On November 17, 2023, Defendant's attorneys moved to withdraw as counsel for Defendant. (ECF No. 50.) Plaintiff did not oppose the motion. (ECF No. 53.) On December 14,

2023, the Court granted Defendant's attorneys' Motion to Withdraw. (ECF No. 58.) Defendant is now proceeding *pro se.* (*Id.* at 2.)

II. LEGAL STANDARD

Preliminary injunctive relief is an "extraordinary remedy, which should be granted only in limited circumstances." *Ferring Pharms., Inc. v. Watson Pharms., Inc.*, 765 F.3d 205, 210 (3d Cir. 2014) (quoting *Novartis Consumer Health, Inc. v. Johnson-Merck Consumer Pharms. Co.*, 290 F.3d 578, 586 (3d Cir. 2002)). The primary purpose of preliminary injunctive relief is "maintenance of the status quo until a decision on the merits of a case is rendered." *Acierno v. New Castle Cnty.*, 40 F.3d 645, 647 (3d Cir. 1994).

In order to obtain a temporary restraining order or preliminary injunction, the moving party must show:

- (1) a reasonable probability of eventual success in the litigation, and
- (2) that it will be irreparably injured . . . if relief is not granted
[In addition,] the district court, in considering whether to grant a preliminary injunction, should take into account, when they are relevant, (3) the possibility of harm to other interested persons from the grant or denial of the injunction, and (4) the public interest.

Reilly v. Cnty. of Harrisburg, 858 F.3d 173, 176 (3d Cir. 2017) (quoting *Del. River Auth. v. Transamerican Trailer Transp., Inc.*, 501 F.2d 917, 919–20 (3d Cir. 1974)).

The movant bears the burden of establishing "the threshold for the first two 'most critical' factors If these gateway factors are met, a court then considers the remaining two factors and determines in its sound discretion if all four factors, taken together, balance in favor of granting the requested preliminary relief." *Id.* at 179. A court may issue an injunction to a plaintiff "only if the plaintiff produces evidence sufficient to convince the district court that all four factors favor preliminary relief." *AT&T v. Winback & Conserve Program*, 42 F.3d 1421, 1427 (3d Cir. 1994); *see also P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504,

508 (3d Cir. 2005) (“The burden lies with the plaintiff to establish every element in its favor, or the grant of a preliminary injunction is inappropriate.”); *Ferring*, 765 F.3d at 210. A preliminary injunction also should not be issued where material issues of fact are in dispute. *Vita-Pure, Inc. v. Bhatia*, Civ. A. No. 14-7831, 2015 WL 1496396, at *3 (D.N.J. Apr. 1, 2015) (denying injunction where factual disputes “preclude a determination that Plaintiffs have established a likelihood of success on the merits”); *Watchung Spring Water Co. v. Nestle Waters N. Am. Inc.*, Civ. A. No. 14-04984, 2014 WL 5392065, at *2 (D.N.J. Oct. 23, 2014), *aff’d*, 588 F. App’x 197 (3d Cir. 2014).

When seeking mandatory injunctive relief that “will alter the status quo, the party seeking the injunction must meet a higher standard of showing irreparable harm in the absence of an injunction.” *Tracey v. Recovco Mortg. Mgmt.*, 451 F. Supp. 3d 337, 341 (D.N.J. 2020) (quoting *Bennington Foods LLC v. St. Croix Renaissance, Grp., LLP*, 528 F.3d 176, 179 (3d Cir. 2008)). Injunctive relief is considered mandatory, rather than prohibitory, when it will “alter the status quo by commanding some positive act.” *Silvertop Assocs., Inc. v. Kangaroo Mfg., Inc.*, 319 F. Supp. 3d 754, 761 (D.N.J. 2018) (quoting *Coast to Coast Entm’t, LLC v. Coastal Amusements, Inc.*, Civ. A. No. 05-3977, 2005 WL 7979273, at *9 (D.N.J. Nov. 7, 2005)). Although the factors for a mandatory preliminary injunction are the same as for a prospective preliminary injunction, the moving party “bears a particularly heavy burden with respect to each of the preliminary injunction factors.” *Am. Fin. Res., Inc v. Nationstar Mortg.*, Civ. A. No. 14-7555, 2016 WL 8201959, at *2 (D.N.J. Apr. 29, 2016) (citing *Advanced Oral Techs., L.L.C. v. Nutrex Rsch., Inc.*, Civ. A. No. 10-5303, 2011 WL 13881, at *2 (D.N.J. Jan. 3, 2011)). Mandatory preliminary injunctions are therefore generally disfavored, *Silvertop*, 319 F. Supp. 3d at 761 (quoting *Coast to Coast*, 2005 WL 7979273, at *9) and granted “sparingly,” *Tracey*, 451 F. Supp. 3d at 341 (quoting *United States v. Spectro Foods Corp.*, 544 F.2d 1175, 1181 (3d Cir. 1976)).

III. DECISION

Plaintiff seeks a mandatory preliminary injunction requiring Defendant to:

- (1) submit all devices, accounts, and hard copy documents in his possession, custody, or control to [Plaintiff]’s forensic vendor to allow all [Plaintiff’s] information to be forensically removed and preserved as evidence; (2) provide to [Plaintiff]’s counsel a complete log of all copies, transfers, and disclosures Defendant has made of [Plaintiff]’s information; and (3) keep [Plaintiff] informed of his home and business address for a period of one year after termination of his employment with [Plaintiff], consistent with his contractual duties, to enable [Plaintiff] to inform Defendant and any new employers of Defendant’s confidentiality obligations.

(ECF No. 31 at 1.) Plaintiff argues this relief is necessary because Defendant is still in possession of Plaintiff’s confidential and proprietary information. (*Id.* at 2–3.) Plaintiff argues Defendant may inadvertently or deliberately release this unsecured information, and the lack of security measures protecting the information increases the likelihood of disclosure. (*Id.*) Plaintiff further asserts it has shown all four of the preliminary injunction factors weigh in its favor, as (1) it has presented clear evidence of Defendant’s misappropriation of trade secrets through emails, photographs, and possession of other proprietary information (*id.* at 13–16), (2) the risk of Defendant deliberately or inadvertently releasing the information to Plaintiff’s competitors constitutes a risk of irreparable harm if the injunction is not granted (*id.* at 16–17), (3) the balance of equities favors the injunction as Defendant has no legitimate interest in retaining Plaintiff’s trade secrets and confidential information (*id.* at 17–18), and (4) the injunctive relief is in the public interest as it ensures the protection of Plaintiff’s legitimate trade secrets (*id.* at 18–19).

Defendant responds that Plaintiff has failed to demonstrate it would suffer irreparable harm absent the injunction, as it has not shown Defendant continues to have any of its information. (ECF No. 40 at 5.) Defendant also asserts an injunction would violate his constitutional right under the Fifth Amendment of the United States Constitution, as producing the documents required by the

injunction would constitute a testimonial act against himself under the act of production doctrine. (*Id.* at 7–10.) Defendant argues producing the information Plaintiff demands would itself constitute testimony that the information exists, particularly because Plaintiff cannot detail with “reasonable particularity” that its “proprietary information actually exists on [Defendant’s] devices, that this information is actually in [Defendant’s] possession, or that it is authentic.” (*Id.* at 9.)

Plaintiff replies that Defendant waived his Fifth Amendment rights when he voluntarily produced his personal laptop and email account to Plaintiff, and Plaintiff already is aware, and has evidence, of Defendant’s possession of the demanded information, both because Defendant signed documents admitting to his wrongdoing, and because Plaintiff has provided specific examples of the information misappropriated by Defendant. (ECF No. 42 at 1, 4–8.)

A. Reasonable Probability of Eventual Success in Litigation

To satisfy the first prong of the preliminary injunction inquiry, a plaintiff must demonstrate a reasonable probability of success on the merits of the action. *Am. Express Travel Related Servs., Inc. v. Sidamon-Eristoff*, 669 F.3d 359, 366 (3d Cir. 2012). At the preliminary injunction stage, a plaintiff need only show a reasonable chance of winning or, in other words, a chance that is “significantly better than negligible but not necessarily more likely than not.” *Reilly*, 858 F.3d at 179.

Plaintiff argues it is likely to succeed on its Defend Trade Secrets Act (“DTSA”) claim because (1) the information allegedly taken is conventional trade secret information (*i.e.*, information linked to the scientific and commercial development of medical therapies), which Plaintiff took extensive steps to protect, (2) the information was to be used in interstate commerce across the United States, and (3) Plaintiff has clear evidence of Defendant’s misappropriation of this information through emails sent to his personal email account and files stored on his personal

computer. (ECF No. 31 at 13–15.) Plaintiff also argues its New Jersey Trade Secrets Act (“NJTSA”), Computer Fraud and Abuse Act (“CFAA”), and conversion claims are likely to succeed for the same reasons. (*Id.* at 14–15.) Defendant does not respond to Plaintiff’s argument regarding likelihood of success on the merits.

“Courts in this district ‘fold’ the DTSA analysis into the NJTSA review,” meaning claims under the two statutes are assessed simultaneously. *Corp. Synergies Grp., LLC v. Andrews*, Civ. A. No. 18-13381, 2019 WL 3780098, at *3 (D.N.J. Aug. 12, 2019) (quoting *Scherer Design Grp., LLC v. Schwartz*, Civ. A. No. 18-3540, 2018 WL 3613421, at *4 (D.N.J. July 26, 2018)). The statutes require a plaintiff “demonstrate (1) the existence of a trade secret, defined broadly as information with independent economic value that the owner has taken reasonable measures to keep secret, and (2) misappropriation of that secret, defined as the knowing improper acquisition and use or disclosure of the secret.” *Par Pharm., Inc. v. QuVa Pharma, Inc.*, 764 F. App’x 273, 278 (3d Cir. 2019).

1. Existence of a Trade Secret

Plaintiff can show the existence of trade secrets because it has demonstrated it holds economically valuable information which it has taken, and is taking, reasonable measures to keep secret. For a plaintiff to sufficiently identify a trade secret, (i) “[t]he allegedly misappropriated trade secret must be identified with enough specificity to place a defendant on notice of the bases for the claim being made against it”; and (ii)

the subject matter of the trade secret must be described with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies.

Oakwood Lab’ys LLC v. Thanoo, 999 F.3d 892, 905 (3d Cir. 2021).

Plaintiff claims Defendant has misappropriated its trade secrets including the “proprietary [REDACTED] for [Plaintiff’s] next generation therapeutic products, data related to proprietary [REDACTED], proprietary manufacturing processes, [REDACTED] for their therapeutic constructs, [REDACTED], and confidential information [REDACTED]” which together “have values greater than [REDACTED].” (ECF No. 30-5 ¶¶ 9–10.) Scientific data for the development of medical treatments is axiomatic trade secret information. *See Par Pharm.*, 764 F. App’x at 278 (“[Plaintiff] demonstrated a reasonable likelihood that the APS Plan was a trade secret. The Plan discloses aspects of [Plaintiff’s] economically valuable FDA-mandated sterile manufacturing procedures.”); *Acteon, Inc. v. Harms*, Civ. A. No. 20-14851, 2020 WL 6694411, at *9 (D.N.J. Nov. 6, 2020) (finding proprietary presentation of R&D partner of medical device company constitutes a trade secret); *Jazz Pharm., Inc. v. Synchrony Grp., LLC*, 343 F. Supp. 3d 434, 444 (E.D. Pa. 2018) (holding “confidential marketing materials, non-public drug sales data and data regarding physician-prescribing habits, analyses of prescriber and patient data commissioned by [plaintiff], marketing research, analyses of its own products compared to other narcolepsy products, and risk evaluation and mitigation strategy research” constitute trade secrets). Moreover, Plaintiff alleges specific documents, including emails containing Plaintiff’s confidential and proprietary information, that Defendant took and sent to his personal email account on various dates. (ECF No. 31 at 5–6.); *see Corp. Synergies Grp.*, 2019 WL 3780098, at *4 (finding Plaintiff sufficiently identified the trade secrets at issue, as it “specifically names and describes documents that [defendant] accessed the day before he resigned from [plaintiff] and that [another defendant] emailed to herself prior to her resignation”).

Plaintiff is also able to show it has taken reasonable steps to keep its confidential and proprietary information secret, claiming it has instituted a “comprehensive computer security

network” including “tightly restricted access, firewalls, private networks, and password protection that effectively safeguard its information, data, and documents.” (ECF No. 31 at 14.) Plaintiff also states it has implemented contractual controls on its employees “to limit their use and authorization to use Plaintiff’s information beyond that which is necessary for their job duties at Plaintiff.” (*Id.*) Such efforts constitute reasonable measures to keep the information secret. *See NJ Coed Sports LLC v. ISP Sports, LLC*, Civ. A. No. 22-06969, 2023 WL 3993772, at *4 (D.N.J. June 14, 2023) (finding that “[n]on-disclosure or confidentiality agreements are often considered ‘reasonable measures’ of keeping information secret under the DTSA”); *Corp. Synergies Grp.*, 2019 WL 3780098, at *4 (finding a corporate data storage policy, including password protected servers, and the acknowledgment and signing of confidentiality agreements, were “reasonable measures” for the protection of trade secrets); *Orient Turistik Magazcilik San ve Tic Ltd. v. Aytek USA, Inc.*, Civ. A. No. 22-4864, 2023 WL 3559049, at *6 (D.N.J. May 18, 2023) (finding plaintiff had taken “reasonable measures” to protect its customer list as it maintained two levels of password protection, limited access to the list, kept the list on a computer disconnected from the internet and printers, and took measures during the shipping process to prevent disclosure of the list). Therefore, the Court finds Plaintiff has demonstrated a reasonable likelihood of the existence of a trade secret and accordingly has shown a reasonable probability of satisfying the first prong in a DTSA and NJTSA claim.

2. Misappropriation

Plaintiff is likely to succeed in demonstrating that Defendant misappropriated its trade secrets, as it details specific emails where Defendant sent proprietary company information to his personal email. (ECF No. 31 at 4–6.) “The DTSA states that ‘misappropriation’ includes ‘acquisition of a trade secret of another by a person who knows or has reason to know that the

trade secret was acquired by improper means[.]” *Shrink Packaging Sys. Corp. v. Kist*, Civ. A. No. 22-04967, 2023 WL 5664733, at *7 (D.N.J. Sept. 1, 2023) (quoting 18 U.S.C. § 1839(5)(A))². Improper means can include “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” *Shrink*, 2023 WL 5664733, at *7 (quoting 18 U.S.C. § 1839(6)). Improper acquisition occurs “when a defendant agreed to abide by a confidentiality agreement but ‘impermissibly sen[ds] the trade secrets to her personal email account in violation of [p]laintiff’s policies and confidentiality agreement.’” *Shrink*, 2023 WL 5664733, at *7 (quoting *Bramshill Invs., LLC v. Pullen*, Civ. A. No. 19-18288, 2020 WL 4581827, at *4 (D.N.J. Aug. 10, 2020)).

Here, Plaintiff has demonstrated a reasonable probability of proving Defendant’s misappropriation of Plaintiff’s trade secrets, as it has alleged and proffered evidence of Defendant emailing Plaintiff’s confidential information to his personal email account. In its briefing, Plaintiff specifically identifies six instances where Defendant emailed Plaintiff’s trade secret data to his personal email account, including emails containing “data regarding the efficacy [REDACTED] [Plaintiff] was considering using to produce its proprietary cell therapy” (ECF No. 31 at 5; ECF No. 30-1), “a . . . [REDACTED]” (ECF No. 31 at 5; ECF No. 30-2 at 1–5), and “slides from a confidential meeting of [Plaintiff’s] research review committee . . . describing [Plaintiff]’s rationale and strategy for how to produce its proprietary cell therapy” (ECF No. 31 at 5; ECF No. 30-2 at 6–14). A defendant sending trade secrets to their personal email account constitutes misappropriation. *Shrink*, 2023 WL 5664733, at *7 (quoting *Bramshill*, 2020 WL 4581827, at *4); see also *Sandhills Glob., Inc. v. Garafola*, Civ. A. No. 19-20669, 2020 WL 4228068, at *3 (D.N.J. July 23, 2020) (finding trade secret misappropriation was sufficiently alleged when plaintiff

² The NJTSA has an identical provision. N.J. Stat. Ann. § 56:15-2(1).

claimed defendant “transmitted to his personal e-mail account proprietary information belonging to” plaintiff); *Chubb Ina Holdings Inc. v. Chang*, Civ. A. No. 16-2354, 2017 WL 499682, at *9 (D.N.J. Feb. 7, 2017) (finding plaintiff sufficiently alleged a DTSA claim where it claimed defendants emailed plaintiff’s confidential information to their personal email accounts). Based on Plaintiff’s allegations and proffered evidence of Defendant sending Plaintiff’s confidential information to his personal email account, the Court finds Plaintiff has demonstrated a reasonable likelihood of showing trade secret misappropriation and accordingly has shown a reasonable probability of satisfying the second prong of a DTSA and NJTSA claim.

Therefore, because Plaintiff has shown it is reasonably likely to succeed on its DTSA and NJTSA claims, the Court concludes Plaintiff has satisfied the first prong of the preliminary injunction inquiry by showing a reasonable probability of success on the merits³.

B. Likelihood of Irreparable Harm to Plaintiff

To satisfy the second prong of the preliminary injunction inquiry, the plaintiff must demonstrate a probability of irreparable harm if the injunction is not granted. *GJ JM Enters., LLC v. City of Atl. City*, 293 F. Supp. 3d 509, 520 (D.N.J. 2017) (quoting *Frank’s GMC Truck Ctr., Inc. v. Gen. Motors Corp.*, 847 F.2d 100, 102 (3d Cir. 1988)). Overall, “[i]n order to demonstrate irreparable harm the plaintiff must demonstrate potential harm which cannot be redressed by a legal or an equitable remedy following a trial. The preliminary injunction must be the only way

³ Plaintiff also brought a CFAA claim (ECF No. 1 ¶¶ 55–61), a claim for breach of its confidentiality agreement with Defendant (*id.* ¶¶ 74–80), and a conversion claim (*id.* ¶¶ 81–88). The Court does not comment on the merits of these claims as they are not essential to the Court’s decision on Plaintiff’s Motion for Preliminary Injunction, given that the requested relief is premised on the protection of Plaintiff’s trade secrets, and the Court has already found the Plaintiff is likely to succeed on its DTSA and NJTSA claims. (ECF No. 31-3) (requesting an injunction to protect “Plaintiff’s trade secrets and confidential information” and prevent their inadvertent use or disclosure).

of protecting the plaintiff from harm.” *GJJM*, 293 F. Supp. 3d at 520 (quoting *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 801 (3d Cir. 1989)). In the context of a preliminary injunction, the Plaintiff must show that irreparable harm would be immediate, as “demonstrating ‘a risk of irreparable harm is not enough.’” *GEODIS USA, LLC v. Bravi*, Civ. A. No. 23-4322, 2023 WL 7221372, at *3 (D.N.J. Nov. 2, 2023) (quoting *Hoxworth v. Blinder, Robinson & Co.*, 903 F.2d 186, 205 (3d Cir. 1990)).

Plaintiff argues it is likely to experience imminent irreparable harm if Defendant continues to maintain possession of its trade secrets on unsecured personal devices because Defendant could release that information to one or more of Plaintiff’s competitors, either deliberately or inadvertently. (ECF No. 31 at 16.) Plaintiff claims it is impossible to quantify the loss that would result from the disclosure of its trade secrets to competitors, who could use the information to harm Plaintiff’s business and goodwill and deprive the trade secrets of all their value. (*Id.* at 16–17.) Plaintiff argues a mandatory injunction is the only way to appropriately mitigate the risk of its trade secrets being disclosed. (*Id.* at 17.)

Defendant claims Plaintiff is unable to establish imminent irreparable harm and is instead seeking a preliminary injunction based on a remote and speculative future injury. (ECF No. 40 at 5–6.) Defendant asserts he is already subject to a TRO that prohibits him from disseminating Plaintiff’s information, and therefore there is no need for further injunctive relief. (*Id.* at 6.) Defendant also argues that Plaintiff has only shown a potential for economic loss which cannot constitute irreparable harm. (*Id.*)

Plaintiff replies that Defendant has shown “he cannot be trusted in this matter” because he emailed Plaintiff’s proprietary information to his personal email account using seemingly innocuous file names. (ECF No. 42 at 2–3.) Plaintiff argues Defendant still has its confidential and

proprietary information unsecured on his personal email accounts and devices, thereby exposing Plaintiff to the risk of that information being disclosed at any time. (*Id.* at 3.) Plaintiff contends Defendant has admitted he is still in possession of its trade secrets, and Plaintiff has identified specific trade secrets still in Defendant's possession. (*Id.* at 3–4.) Plaintiff argues it is being presently harmed by Defendant's continued possession of the trade secrets and that irreparable harm would occur if its trade secret information is disclosed, since the value of its trade secrets would be lost forever. (*Id.*)

It is well-established that the potential disclosure of a plaintiff's trade secrets constitutes a potential for irreparable harm, as the value of a trade secret is lost entirely once disclosed. *Jackson Hewitt, Inc. v. DJSG Utah Tax Serv., LLC*, Civ. A. No. 10-05108, 2011 WL 90311, at *6 (D.N.J. Jan. 10, 2011) (finding that “[w]here a party is in possession of another party's confidential information and is poised to use or disclose such information, there is a likelihood of irreparable harm”); *Nat'l Reprographics, Inc. v. Strom*, 621 F. Supp. 2d 204, 229 (D.N.J. 2009) (finding potential disclosure of plaintiff's information to competitor sufficient to demonstrate irreparable harm, as “[t]here is no question that using [plaintiff's] confidential information and proprietary information for the benefit of its competitors could potentially destroy [plaintiff's] business, built over 100 years”); *Neo Gen Screening, Inc. v. TeleChem Intern., Inc.*, 69 F. App'x 550, 554–55 (3d Cir. 2003) (citing *FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir.1984)) (holding that a loss of trade secrets was an irreparable harm that could not be measured in money because “a trade secret once lost is, of course, lost forever”). Therefore, any evidence that Defendant may potentially disclose Plaintiff's trade secrets would weigh in favor of finding irreparable harm.

Defendant's past conduct regarding Plaintiff's trade secrets is relevant in considering whether injunctive relief is warranted. Courts in this district have granted injunctive relief against defendants based on prior wrongful conduct regarding a plaintiff's assets or trade secrets. *See Wilmington Sav. Fund Soc'y v. Otieno-Ngoje*, Civ. A. No. 16-5631, 2016 WL 6821086, at *1–2 (D.N.J. Nov. 17, 2016) (granting preliminary injunction placing constructive trust and equitable lien on insurance funds in defendant's possession because “[p]laintiff has clearly shown that Defendant has already dissipated a portion of the funds subject to a potential judgment”); *Ameriprise Fin. Servs., Inc. v. Koenig*, Civ. A. No. 11-6140, 2012 WL 379940, at *7 (D.N.J. Feb. 6, 2012) (finding irreparable harm and granting plaintiff preliminary injunction compelling defendant to return confidential information based on evidence defendant had taken information beyond what was authorized); *Esquire Deposition Servs., LLC v. Boutot*, Civ. A. No. 09-1526, 2009 WL 1812411, at *8–9 (D.N.J. June 22, 2009) (finding a likelihood of irreparable harm where plaintiff discovered defendant's possession of confidential information via circumstantial information, as defendant was using the information to identify and email plaintiff's competitors). Therefore, Plaintiff's proffered evidence of Defendant sending its trade secrets to his personal email account is relevant in assessing Plaintiff's risk of irreparable harm.

Furthermore, courts have found that a plaintiff may suffer irreparable harm if confidential information belonging to a plaintiff is not promptly returned. *See Ameriprise*, 2012 WL 379940, at *7 (ordering return of confidential information due to risk of irreparable harm from potential disclosure of information); *Freedom Med. Inc. v. Whitman*, 343 F. Supp. 3d 509, 517 (E.D. Pa. 2018) (noting previous court order requiring defendants to immediately return any “confidential or proprietary information of [p]laintiff that is in their possession or control, in whatever form that information exists”); cf. *Maximum Quality Foods, Inc. v. DiMaria*, Civ. A. No. 14-6546, 2014 WL

6991967, at *4 (D.N.J. Dec. 10, 2014) (finding irreparable harm was not shown where defendant “complied with the Court’s Order and returned the confidential information at issue to [p]laintiff”).

Therefore, if Plaintiff can demonstrate it is probable Defendant is still in possession of its confidential and proprietary information, it will be able to show a probability of irreparable harm.

The Court finds Plaintiff has shown a probability of irreparable harm that warrants the removal of Plaintiff’s secret and confidential information from Defendant’s devices and possession, as it has presented evidence indicating Defendant is still in possession of its confidential information, and Defendant may inadvertently or deliberately release this unsecured information to one or more of Plaintiff’s competitors and/or may use this information to seek alternate employment, particularly given Defendant has already contacted other employers about developing competing cell therapy businesses. (ECF No. 31 at 8.) As discussed above, Plaintiff specifically identifies six instances where Defendant emailed trade secret data to his personal email account, including emails containing “data regarding the efficacy of [REDACTED] [Plaintiff] was considering using to produce its proprietary cell therapy” (ECF No. 31 at 5; ECF No. 30-1), “a . . . [REDACTED]” (ECF No. 31 at 5; ECF No. 30-2 at 1–5), and “slides from a confidential meeting of [Plaintiff’s] research review committee . . . describing [Plaintiff]’s rationale and strategy for how to produce its proprietary cell therapy” (ECF No. 31 at 5; ECF No. 30-2 at 6–14). Defendant also signed the “Certification of Document Destruction Compliance Certificate” where he indicated he “routinely emailed [Plaintiff’s] confidential and proprietary information and documents to [his] personal email address lianxing.liu@gmail.com, which emails [he] understand[ed] are also saved on and/or accessible by [his] personal smart phone and [his] personal computer.” (ECF No. 31 at 6.) Plaintiff also presented evidence that, when inspecting Defendant’s personal laptop, it discovered “the ‘trash’ was emptied on May 16 at about 4:00 pm, just after

[Plaintiff] requested that [Defendant] bring the personal laptop to the Piscataway office.” (*Id.* at 7.) Defendant’s continued possession of the information was corroborated by evidence “Defendant had stored on his personal iPhone multiple photos of [Plaintiff’s] slides marked as privileged, confidential, and for internal use only” among other documents stored on personal devices. (*Id.* at 7–8.) Finally, Plaintiff has proffered evidence of Defendant’s messages to Plaintiff’s competitors offering to help such competitors develop cell therapy businesses and products related to the trade secrets Defendant allegedly took. (*Id.* at 8.) By providing this evidence, Plaintiff has shown a high probability Defendant continues to possess Plaintiff’s trade secrets, and that Defendant may disclose such trade secrets to Plaintiff’s competitors. The evidence of Defendant’s possession of trade secrets, and of Defendant’s intent to disclose the trade secrets to Plaintiff’s competitors, constitutes a potential for irreparable harm that warrants the removal of Plaintiff’s trade secrets from Defendant’s devices. *See Ameriprise*, 2012 WL 379940, at *2–7 (ordering return of confidential information based on evidence plaintiff’s confidential information had been deleted from defendant’s personal computer); *Jackson Hewitt*, 2011 WL 90311, at *6 (finding that “[w]here a party is in possession of another party’s confidential information and is poised to use or disclose such information, there is a likelihood of irreparable harm”); *NVR, Inc. v. Davern*, Civ. A. No. 15-5059, 2015 WL 9450831, at *2 (D.N.J. Dec. 23, 2015) (“A party may not defeat an otherwise proper application for an injunction by merely abandoning conduct that if continued or completed would have constituted irreparable harm.”); *Cabela’s LLC v. Highby*, 362 F. Supp. 3d 208, 224 (D. Del. 2019) (finding plaintiff evidenced irreparable harm by showing “that [d]efendants likely obtained and intended to misuse confidential information”).

The Court does not find, however, that it is necessary for Defendant to “provide to [Plaintiff’s] counsel a complete log of all copies, transfers, and disclosures Defendant has made of

[Plaintiff's] information" (ECF No. 31 at 11) at this time, because Plaintiff has not presented any evidence that any transfers or disclosures have actually happened, and the deletion and preservation of the Defendant's copies of secret information by the forensic vendor will suffice to protect Plaintiff from the potential of future disclosure. A preliminary injunction is meant to provide the moving party protection against imminent future harm, not to be used as a discovery tool to find evidence of past harm. *See TriFound Fin., LLC v. Greenberg*, Civ. A. No. 20-19303, 2021 WL 194763, at *5 (D.N.J. Jan. 20, 2021) ("The irreparable harm inquiry concerns threat of future harm, not past harm."); *Gentile v. Sec. & Exch. Comm'n*, Civ. A. No. 19-5155, 2019 WL 109106, at *3 (D.N.J. Mar. 8, 2019) (quoting *Campbell Soup Co. v. ConAgra, Inc.*, 977 F.2d 86, 91 (3d Cir. 1992)) ("The Third Circuit has long distinguished between a showing of immediate irreparable harm, which justifies the issuance of a preliminary injunction, and circumstances in which 'other remedies such as money damages are adequate to compensate a plaintiff for past harm.'"); *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 801 (3d Cir. 1989) ("In order to demonstrate irreparable harm the plaintiff must demonstrate potential harm which cannot be redressed by a legal or an equitable remedy following a trial."). Here, it would be inappropriate for the Court to order Defendant to provide Plaintiff information about past harm, particularly when Plaintiff has demonstrated no immediate need for this information to prevent future harm.

The Court also finds Plaintiff has not demonstrated a potential for irreparable harm to compel Defendant to provide his home and business address to Plaintiff for one year, as Plaintiff has not presented any argument for why it would be irreparably harmed should this relief not be granted. Although Plaintiff has alleged that Defendant is contractually obligated to keep them informed of his home and business addresses (ECF No. 31 at 10), a breach of contract allegation is insufficient to show irreparable harm. *See Hit Dr. Tri State Arsenal v. Barth*, Civ. A. No. 19-

14579, 2020 WL 729152, at *8 (D.N.J. Feb. 11, 2020) (“Just because a contract includes [a] term doesn’t bootstrap a contractual breach into irreparable harm.”); *Interlink Grp. Corp. USA, Inc. v. Am. Trade & Fin. Corp.*, Civ. A. No. 12-6179, 2013 WL 1811898, at *3 (D.N.J. Apr. 25, 2013) (quoting *Continental Grp., Inc. v. Amoco Chems. Corp.*, 614 F.2d 351, 358 (3d Cir. 1980) (a preliminary injunction cannot be granted to allay the “fears and apprehensions” of the mover); *431 E Palisade Ave. Real Est. v. City of Englewood*, Civ. A. No. 19-14515, 2019 WL 5078865, at *12 (D.N.J. Oct. 10, 2019), *rev’d on other grounds*, 977 F.3d 277 (holding “breach-of-contract damages can be readily addressed following a trial”). Therefore, Plaintiff has not shown a potential for irreparable harm from Defendant not providing his addresses to them.

Therefore, the Court concludes Plaintiff has demonstrated a probability of irreparable harm justifying the removal and preservation of its trade secrets by a forensic vendor and accordingly satisfies the second prong of the preliminary injunction inquiry.

C. Balance of Equities

The third prong of the preliminary injunction inquiry requires the Court to balance the equities between Plaintiff and Defendant by “balanc[ing] the harm that will occur to the moving party from the denial of the preliminary injunction with the harm that the non-moving party will incur if the injunction is granted.” *Power Surv., LLC v. Premier Util. Servs., LLC*, 61 F. Supp. 3d 477, 487 (D.N.J. 2014).

Plaintiff argues Defendant will not be harmed by mandatory injunctive relief, as he has no legitimate interest in retaining Plaintiff’s trade secret and confidential information and is in any case contractually obligated to provide certain aspects of the relief requested due to his confidentiality agreement with Plaintiff. (ECF No. 31 at 17.) Plaintiff claims it, on the other hand, would suffer significant harm due to the potential irreparable harm previously detailed. (*Id.* at 17–

18.) On the Fifth Amendment issue, Plaintiff argues that Defendant waived his Fifth Amendment protections when he voluntarily produced his personal devices and accounts to Plaintiff. (*Id.* at 19–20.) Plaintiff also argues that the fact Defendant has Plaintiff’s secret information is a foregone conclusion, as Defendant has already admitted to the theft of trade secrets in Court and in a signed document, and Plaintiff has also reviewed Defendant’s personal devices and accounts during the previous voluntary production that indicate he still has Plaintiff’s trade secrets in his possession. (*Id.* at 20–21.)

Defendant argues he would be subject to significant harm because mandatory injunctive relief would violate his Fifth Amendment rights. (ECF No. 40 at 6–7.) Defendant argues that producing his personal devices, online accounts, and documents to Plaintiff’s forensic vendor, and providing Plaintiff’s counsel a log of all copies, transfers, and disclosures of Plaintiff’s confidential and trade secret information would violate his Fifth Amendment right against self-incrimination. (*Id.* at 6–8.) Defendant argues his production of the requested documents would constitute an act of production, as the production of the documents would admit their existence and Defendant’s possession and control of them, thereby exposing him to potential criminal sanction. (*Id.* at 7–8.) Defendant also argues the foregone conclusion doctrine does not apply in this case as Plaintiff cannot identify with “reasonable particularity” the specific information Defendant possesses, or its authenticity. (*Id.* at 9.) Rather, Defendant contends Plaintiff is requesting injunctive relief to determine whether Defendant still possesses any of Plaintiff’s information. (*Id.*) As a result, the mandatory injunction should not issue due to Defendant’s Fifth Amendment rights. (*Id.*)

Plaintiff responds that Defendant waived his Fifth Amendment rights by voluntarily producing his personal devices to Plaintiff during its internal investigation. (ECF No. 42 at 5.) Plaintiff also argues that the mere possibility of a criminal investigation would not constitute

irreparable harm to Defendant. (*Id.* at 4–5.) On the substance of Defendant’s Fifth Amendment arguments, Plaintiff asserts that Defendant’s potential production in this case would not be testimonial, as Defendant has already admitted to possessing Plaintiff’s information in a signed compliance certificate, and because Plaintiff has identified specific trade secrets Defendant possesses. (*Id.* at 5–7.) Plaintiff states the foregone conclusion doctrine applies when the existence and possession of records is already known, and there is no need for Plaintiff to specify the contents of the information it wants produced. (*Id.* at 7–8.)

The Fifth Amendment protects against self-incrimination through its provision that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” U.S. Const. amend. V. The Fifth Amendment is to be construed liberally to protect the rights it was intended to secure. *Sallah v. Worldwide Clearing LLC*, 855 F. Supp. 2d 1364, 1369 (S.D. Fla. 2012) (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951)); *see also United States v. Radchik*, Civ. A. No. 171187, 2017 WL 2380177, at *3 (D.N.J. June 1, 2017). To claim the protection of the Fifth Amendment, the proponent must show a “substantial and real hazard of self-incrimination.” *Sallah*, 855 F. Supp. 2d at 1369 (quoting *United States v. Argomaniz*, 925 F.2d 1349, 1353 (11th Cir.1991)); *see also Radchik*, 2017 WL 2380177, at *3 (“[t]he protection is limited to instances ‘where the witness has reasonable cause to apprehend danger from a direct answer.’”). The Fifth Amendment does not bar the production of all incriminating evidence, “but applies only when the accused is compelled to make a Testimonial Communication that is incriminating.” *United States v. Apple MacPro Comput.*, 851 F.3d 238, 247 (3d Cir. 2017) (quoting *Fisher v. United States*, 425 U.S. 391, 408 (1976)). “To be testimonial, a communication must either ‘explicitly or implicitly . . . relate a factual assertion or disclose information.’” *Apple*, 851 F.3d at 247 (quoting *Doe v. United States*, 487 U.S. 201, 210 (1988)). The Fifth Amendment may

be asserted in civil proceedings if an individual “reasonably believes his answers could be used in a criminal prosecution or lead to other evidence that could be used in a criminal prosecution.” *KST Data, Inc. v. DXC Tech Co.*, Civ. A. No. 17-7927, 2018 WL 5776842, at *1 (C.D. Ca. Oct. 15, 2018).

An act of production can have testimonial impacts which infringe on the producer’s Fifth Amendment rights, because “[t]he ‘act of producing documents in response to a subpoena may have a compelled testimonial aspect [because by] producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.’” *In re Reliant Energy Erisa Litig.*, Civ. A. No. 02-2051, 2005 WL 8166073, at *2 (S.D. Tex. Jan. 28, 2005) (quoting *United States v. Hubbell*, 530 U.S. 27, 36 (2000)). The foregone conclusion exception allows a proponent to compel production when “[t]he existence and location of the [documents] are a foregone conclusion and the [producer] adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the [documents].” *United States v. Friedman*, 337 F. Supp. 3d 259, 265 (S.D.N.Y. 2018). For the exception to apply, the proponent “need not demonstrate perfect knowledge of each specific responsive document,” but it must “know, and not merely infer, that the sought documents exist, that they are under the control of defendant, and that they are authentic.” *Id.* The proponent of the production must, therefore, be able to specifically identify each of the documents it is seeking but need not identify the contents of those documents. *United States v. Greenfield*, 831 F.3d 106, 116 (2d Cir. 2016) (quoting *Hubbell*, 530 U.S. at 44–45).

To show a waiver of a defendant’s Fifth Amendment rights, the proponent must show the waiver was “knowing, intelligent, and voluntary under the ‘high standar[d] of proof for the waiver of constitutional rights.’” *United States v. Restitullo*, 215 F. Supp. 3d 343, 352 (D.N.J. 2016)

(quoting *Maryland v. Shatzer*, 559 U.S. 98, 104 (2010)). “[F]ederal courts have uniformly held that, where criminal facts have been voluntarily revealed, the privilege cannot be invoked to avoid disclosure of the details.” *Ameriprise Fin. Servs., Inc. v. Koenig*, Civ. A. No. 11-6140, 2012 WL 693042, at *3. When a party “objects to testifying or producing discovery based on their privilege against self-incrimination, that objection must be made in a timely manner.” *Brown v. Caldwell*, Civ. A. No. 20-07907, 2022 WL 2753243, at *2 (D.N.J. July 14, 2022). The Fifth Amendment is not “self-executing and thus must be claimed when self-incrimination is threatened.” *United States v. Frierson*, 945 F.2d 650, 660 (3d Cir. 1991).

Plaintiff’s proposed injunctive relief against Defendant would compel a testimonial production by Defendant, as Defendant’s production of his devices, accounts, and documents to a forensic vendor could potentially reveal his possession and control of incriminating documents. See *United States v. Apple MacPro Comput.*, 851 F.3d 238, 247 (3d Cir. 2017) (quoting *Fisher*, 425 U.S. at 410) (compliance with a request for evidence may be testimonial as it “may ‘tacitly concede[] the existence of the documents demanded and their possession and control by the [defendant]’”). Theft of trade secrets may carry criminal penalties under Section 1832 of Title 18 of the U.S. Code, which states, in part:

Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information

. . . shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S. Code § 1832(a); *see also United States v. Hou*, Crim. A. No. 20-780, 2022 WL 2671130, at *1 (D.N.J. July 11, 2022) (detailing guilty plea of defendant to one count information under 18 U.S.C. § 1832(a)(3) for copying and removing “thousands of digital files containing proprietary information from [his former employer]”); *Liu v. United States*, Civ. A. No. 17-7041, 2021 WL 3732879, at *1 (D.N.J. Aug. 23, 2021) (noting “Petitioner was also charged with one count of possessing stolen trade secrets in violation of 18 U.S.C. § 1832(a)(3), as he was found to be in possession of trade secrets owned by his former employer in the form of a binder containing documents”). There is a substantial risk that Defendant will disclose incriminating information should he submit his devices, accounts, and documents to a forensic vendor, as this disclosure would create and preserve evidence of trade secrets misappropriated by Defendant. Therefore, because Defendant could be criminally charged if Plaintiff’s trade secrets are found in his possession, and the proposed mandatory injunctive relief would reveal whether such secrets are in fact in his possession, Defendant “reasonably believes his answers could . . . lead to [] evidence that could be used in a criminal prosecution” *KST*, 2018 WL 5776842, at *1, and may theoretically assert the Fifth Amendment in this case. *See U.S. ex rel. DRC, Inc. v. Custer Battles, LLC*, 415 F. Supp. 2d 628, 633 (E.D. Va. 2006) (“A valid assertion of the privilege requires only the existence of a plausible possibility that the person might be prosecuted in this country.”); *Smith v. Harris*, Civ. A. No. 18-2836, 2022 WL 783332, at *5 (D. Md. Mar. 15, 2022) (same).

Here, the issue of waiver bars Defendant from invoking the Fifth Amendment to shield against the mandatory injunctive relief Plaintiff is seeking, because he has voluntarily revealed incriminating facts but is now trying to use the Fifth Amendment to “avoid disclosure of the details.” *Ameriprise*, 2012 WL 693042, at *3. Defendant signed a document indicating he “routinely emailed [Plaintiff]’s confidential and proprietary information and documents to [his]

personal email address lianxing.liu@gmail.com, which emails [he] understand are also saved on and/or accessible by [his] personal smart phone and [his] personal computer,” among other admissions. (ECF No. 30-6 ¶ 1.) Defendant confirmed to the Court that this document was signed voluntarily. (Tr. (ECF No. 8) at 23:4–23:24.) Furthermore, at that time, Defendant did not raise any questions regarding the contents of the document. (*Id.*) The Court therefore finds Defendant signed this document knowingly, intelligently, and voluntarily, and Defendant has not argued otherwise as regards this document. By signing this document, Defendant admitted to incriminating facts including unauthorized possession of Plaintiff’s confidential and proprietary information and emailing that information to his personal email account. He cannot now seek to “avoid disclosure of the details” of the activities he voluntarily admitted to. *Ameriprise*, 2012 WL 693042, at *3. The Court therefore finds Defendant’s knowing, intelligent, and voluntary admission to incriminating facts constitutes a waiver of his Fifth Amendment rights, and accordingly Defendant cannot invoke the Fifth Amendment to shield against the injunctive relief Plaintiff is seeking.

Even if the Court found Defendant did not waive his Fifth Amendment rights, the Court would still find the Fifth Amendment inapplicable in this case due to the foregone conclusion doctrine, as Plaintiff has identified with reasonable particularity the documents it believes Defendant possesses. In its briefing, Plaintiff identifies six instances where Defendant emailed trade secret data to his personal email account, including emails containing “data regarding the efficacy [REDACTED] [Plaintiff] was considering using to produce its proprietary cell therapy” (ECF No. 31 at 5; ECF No. 30-1), “a . . . [REDACTED]” (ECF No. 31 at 5; ECF No. 30-2 at 1–5), and “slides from a confidential meeting of [Plaintiff’s] research review committee . . . describing [Plaintiff]’s rationale and strategy for how to produce its proprietary cell therapy” (ECF

No. 31 at 5; ECF No. 30-2 at 6–14). Plaintiff also indicates knowledge of an additional seventy-four emails sent from Defendant’s company email account to his personal email account, with such emails containing “proprietary [REDACTED], unpublished R&D data, internal presentations, [REDACTED], and third-party confidential information.” (ECF No. 31 at 6.) Plaintiff also notes “Defendant had stored on his personal iPhone multiple photos of [Plaintiff’s] slides marked as privileged, confidential, and for internal use only” among other documents stored on personal devices. (*Id.* at 7–8.) Plaintiff has therefore identified with reasonable particularity numerous documents that it believes are still in Defendant’s possession, making the existence of these documents a foregone conclusion. *Fridman*, 337 F. Supp. 3d at 265 (finding “[t]he existence and location of the [documents] are a foregone conclusion and the [producer] adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the [documents]”); *Greenfield*, 831 F.3d at 116 (holding that the proponent of the production must be able to specifically identify each of the documents it is seeking but need not identify the contents of those documents); *United States v. Gendreau*, Civ. A. No. 12-303, 2014 WL 464754, at *4–5 (S.D.N.Y. Jan. 22, 2014) (finding that the proponent has met the requirements of the foregone conclusion doctrine when it can “demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents”).

As discussed, the harm to Plaintiff is substantial and irreparable due to the potential loss of the entire value of its trade secrets should Defendant intentionally or inadvertently disclose them to competitors, which tips the balance of equities in Plaintiff’s favor. *See GlaxoSmithKline, LLC v. Brooks*, Civ. A. No. 22-00364, 2022 WL 463070, at *4 (D. Md. Feb. 15, 2022) (finding plaintiff had a legitimate “interest in confirming that any misappropriated data has been removed from [defendant’s] personal accounts and devices”); *Hampton Rds. Connector Partners v. Land to Site*

Servs., Inc., Civ. A. No. 23-174, 2023 WL 8539536, at *10 (E.D. Va. Oct. 17, 2023) (noting court’s “preference” for protecting trade secrets); *Brightview Grp., LP v. Teeters*, 441 F. Supp. 3d 115, 141 (D. Md. 2020) (finding potential for irreparable harm from disclosure of trade secrets tipped balance of equities in Plaintiff’s favor). Because the Court concludes Defendant waived his Fifth Amendment rights, the foregone conclusion exception applies, and Plaintiff faces irreparable harm absent a mandatory injunction, the Court finds the balance of the equities weighs in favor of granting Plaintiff’s proposed mandatory injunctive relief. Accordingly, the Court concludes the third prong of the preliminary injunction inquiry weighs in favor of granting the requested injunctive relief.

D. Public Interest

The final prerequisite for granting a preliminary injunction is that the injunction must be in the public interest. *Carlini v. Velez*, 947 F. Supp. 2d 482, 488 (D.N.J. 2013). The public interest factor generally requires the Court to consider the consequence for the broader public of issuing the requested injunction. *GJIM*, 293 F. Supp. 3d at 521.

Plaintiff argues its proposed mandatory injunction is in the public interest because it enforces Defendant’s confidentiality agreement and protects Plaintiff’s legitimate trade secrets and confidential information from disclosure or misuse. (ECF No. 31 at 18–19.) Defendant does not directly address this factor but does note that the Fifth Amendment is an integral part of the legal system. (ECF No. 40 at 2.)

The Court finds the public interest weighs in favor of Plaintiff’s requested mandatory injunctive relief, as it is well-established the public interest favors the enforcement and protection of trade secrets and confidentiality agreements. See *Payroll Assocs., LLC v. AdaptaSoft, Inc.*, Civ. A. No. 12-6375, 2012 WL 12888566, at *2 (D.N.J. Oct. 24, 2012) (quoting *Bimbo Bakeries USA*,

Inc. v. Botticella, 613 F.3d 102, 119 (3d Cir. 2010)) (noting “[t]he Third Circuit expressly recognizes ‘a general public interest in the upholding the inviolability of trade secrets and enforceability of confidentiality agreements’”); *Cherry Hill Programs, Inc. v. Sullivan*, Civ. A. No. 21-20248, 2022 WL 1094254, at *5 (D.N.J. Apr. 12, 2022) (stating “[t]here is a recognized interest in the Third Circuit in upholding trade secrets”); *Acteon*, 2020 WL 6694411, at *12 (quoting *Bimbo*, 613 F. 3d at 119) (holding “there is a generalized public interest in upholding the inviolability of trade secrets and enforceability of confidentiality agreements”). Conversely, although there is a general interest in preserving Fifth Amendment rights, the Fifth Amendment, as noted above, does not shield Defendant in this particular case due to waiver and the foregone conclusion exception.

For these reasons, the Court finds the public interest weighs in favor of granting Plaintiff’s proposed mandatory injunctive relief. Accordingly, the Court concludes the fourth and final prong of the preliminary injunction inquiry weighs in favor of granting the requested injunctive relief.

IV. CONCLUSION

For the reasons set forth above, Plaintiff’s Motion for Preliminary Injunction (ECF Nos. 29–31) is **GRANTED**. An appropriate Order follows.

Date: March 4, 2024

/s/ Brian R. Martinotti
HON. BRIAN R. MARTINOTTI
UNITED STATES DISTRICT JUDGE